



Battlespace Systems Support Directorate Bulletin

(Formerly the "A/IEW Bulletin")



"Serving the Needs of the Battlespace Systems Community"

Volume 1, Issue 2

November 2002

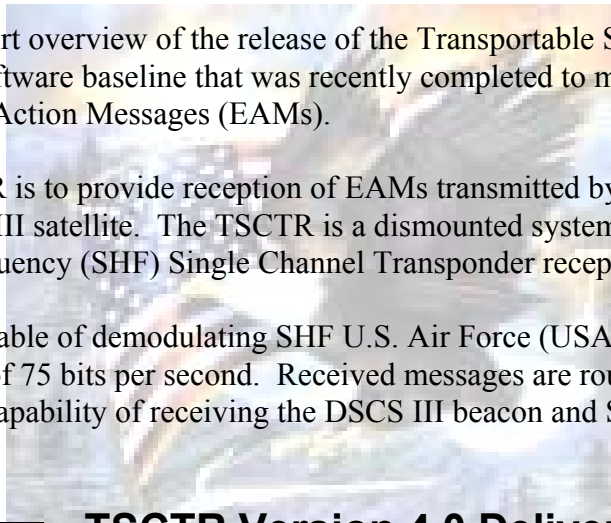
Transportable Single Channel Transponder Receiver Version 4.0 Delivery

Introduction

This article provides a short overview of the release of the Transportable Single Channel Transponder Receiver (TSCTR) Version 4.0 software baseline that was recently completed to meet the requirements of the Warfighter to receive Emergency Action Messages (EAMs).

The mission of the TSCTR is to provide reception of EAMs transmitted by the Defense Satellite Communications System (DSCS) III satellite. The TSCTR is a dismounted system that needs only external power to provide Super High Frequency (SHF) Single Channel Transponder reception.

The TSCTR system is capable of demodulating SHF U.S. Air Force (USAF) Satellite Communications (SATCOM) II messages at a rate of 75 bits per second. Received messages are routed to a printer for hard-copy output. The system provides the capability of receiving the DSCS III beacon and SHF downlink for EAM reception.



TSCTR Version 4.0 Delivery

Work on the enhancements provided by Version 4.0 began in December 2000 and was completed in February 2002, ahead of schedule and under budget. Full software release was approved by CG, CECOM on 11 March 2002.

The following is a summary of the enhancements in the TSCTR Version 4.0 baseline:

- *Enhanced permanent storage save.* Because of the changed security classification guidelines, the TSCTR now saves KI-6 Change-Over Time, Satellite Modifier and Link Modifier in non-volatile memory.

(cont'd page 3)

In This Issue

TSCTR Version 4.0	1
From the Chief	2
SCS/DSCS	3
FLAP/AHUD	4
Bad UDMs	6
ABCS Capabilities	7
ARAT (Re)Introduction	10
For Your Information	15
POC Information	16

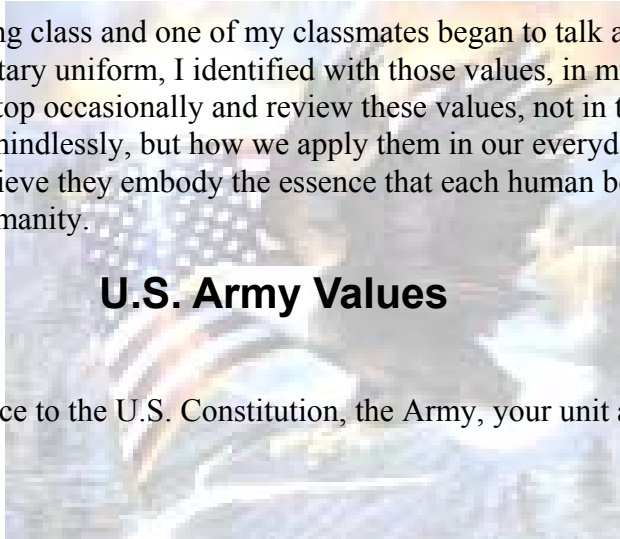
From the Senior Editor's Desk

Written by Mr. Joseph Ingrao, Deputy Director, (A), Battlespace Systems Support



No other nation on earth has consistently portrayed humanity in the way the United States of America has. Each year that goes by, America learns from its mistakes and applies those lessons to ensure she mitigates the opportunity for those mistakes to reoccur. Through the values that we live by, the United States teaches tolerance, and whenever possible finds ways to resolve conflicts non-violently. What other nation on earth can claim to do the same thing? The answer is that very few have been able to claim this honor. Despite some people's assessment that our society values are in a decline, I feel that America will never die, not as long as there are people who care about morals and values and accept others in spite of their differences.

I recently attended a training class and one of my classmates began to talk about the Army values. Although I have never worn a military uniform, I identified with those values, in my work, as well as in my personal life. Everyone needs to stop occasionally and review these values, not in the sense of memorizing them or being able to recite them mindlessly, but how we apply them in our everyday lives. Although they are called the U.S. Army Values, I believe they embody the essence that each human being is capable of and must embrace to ensure the future of humanity.



U.S. Army Values

Loyalty

Bear true faith and allegiance to the U.S. Constitution, the Army, your unit and other soldiers.

Duty

Fulfill your obligations.

Respect

Treat people as they should be treated.

Selfless-Service

Put the welfare of the nation, the Army and your subordinates before your own.

Honor

Live up to all the Army values.

Integrity

Do what's right, legally and morally.

Personal Courage

Face fear, danger, or adversity (Physical or Moral).

“When your values are clear to you, making decisions becomes easier.”

Roy Disney, English Politician

TSCTR (cont'd)

- **Allow reprint of messages.** The TSCTR now supports the reprint of EAMs, at operator command.
- **Reconstruction of messages.** SATCOM II messages are repeated several times to increase the probability that they will be correctly received. The TSCTR is now able to reconstruct the original message from individual blocks, as long as at least one copy of each block is received.
- **Suppress multiple printing of messages.** The TSCTR is now able to recognize that a repeated message has been received so that only one copy is printed.
- **EEPROM Storage Timing Reduction.** The TSCTR keypad freezes while NVRAM is updated. The enhancement for Version 4.0 reduces the save time from ten seconds to four.
- **Reduced print time.** Version 4.0 takes advantage of features of the Miltope Thermal Printer to reduce the time needed for EAM print by 20 seconds.
- **Reduce ROM utilization.** Increased coding efficiency cuts the number of memory chips needed for version release in half.
- **Enhanced KI Change-Over Time Entry.** As a convenience to the users, the TSCTR now defaults the KI-Change-Over Time to 23:59:59 on the 31st. Use of the default avoids acquisition problems that occurred when the field was omitted.

CECOM SEC Communications Software Engineering Support Division provides software support and maintenance for the TSCTR.

For additional information, please contact:

AMSEL-SE-WS-COM (T. Fung), DSN-992-3932, Thomas.fung@mail1.monmouth.army.mil

Submitted by Mr. Thomas Fung, CECOM SEC

Post Production Software Support on the Satellite Communications Set and the Defense Satellite Communications System Electronic Counter-Counter Measures Control Subsystem and Contingency DECS Systems

The AN/USC-28(V) Satellite Communications Set (SCS) operates over the Defense Satellite Communications System (DSCS) Phase II and III satellites. It is an Electronic Counter-Counter Measures (ECCM) communications system that provides jam resistant, secure communication for departmental user networks by employing code division spread spectrum modulation techniques. There are presently two

(cont'd next page)

SCS/DSCS (cont'd)

AN/USC-28(V) hardware configurations: the Airborne and Ground versions. Each version uses a mitigated waveform that allows for maintaining communications in the presence of signal propagation anomalies caused by high altitude nuclear detonation, both during and after the event.

The DSCS ECCM Control Subsystem (DECS) consists of three subsystems: the DECS-Remote Control (DECS-RC), the DECS-Central Control and the Contingency DECS (CDECS). The DECS-RC has a direct interface to the AN/USC-28(V) to automate control of selected functions resulting in enhanced performance of the SCS network that would not be feasible under manual operation. The DECS/CDECS enhances the anti-jam performance of the ECCM network by automatically optimizing AN/USC-28(V) communications links in response to the detection and characterization of enemy jamming signals. The DECS/CDECS reduces operator personnel requirements at both the central and remote locations by automatically collecting the operational status of each AN/USC-28(V) participating in the ECCM network and summarizing this data for the central site network controller.

The latest AN/USC-28(V) software version was the Ground Mitigated Program 7.03, which was fielded in October 2001. This software version corrected 14 reported problems that were investigated, duplicated, corrected, tested and fielded. Seven of the problems dealt directly with improving operator efficiency and the remaining seven corrected internal system problems.

The seven operator reported anomalies that were corrected included: operator COMSEC entry problems, operator emergency receiver messages problem and excessive operator actions. The seven internal system problems eliminated the system and operator notification errors and allowed system testing to be performed more efficiently.

SEC is presently working on the development of the DECS/CDECS Delivery 7 software and new versions of AN/USC-28(V). The Defense Information Systems Agency and the U.S. Army Space Command directed the CECOM SEC to implement 12 Software Change Requests (SCRs) into DECS/CDECS Delivery 7 software release and 31 SCRs into DECS/CDECS Delivery 8 software release. SEC is planning for future AN/USC-28(V) changes to include 22 SCRs in the AN/USC-28(V) Airborne version software release and 26 SCRs in the Ground version software release. These future software releases will reduce operator or network system errors, increase system performance reliability, reduce network entry problems, reduce or eliminate loss of network communications and improve network communication efficiency.

Submitted by Mr. Alan Marchalonis, CECOM SEC

Software Engineering Center Continues to Enhance Its Maintenance Role

The U.S. Army Communications and Electronics Command Software Engineering Center (SEC), Fort Monmouth, NJ, recently developed a support tool called the 'Fault Log Analyzer Program' (FLAP) for the Advanced Aviator's Night Vision Imaging System/Heads-Up Display (AHUD). SEC has the responsibility

(cont'd next page)

FLAP (cont'd)

for performing Life Cycle Software Engineering Support (LCSES) for all United States Army computer-based battlefield systems. LCSES is the overall system support necessary to develop, sustain, modify, refine and improve software for the computer-based battlefield systems, including computer code, databases, documentation and other support software and hardware components.

The AHUD was developed to improve combat and assault military helicopter operations and survivability on the modern battlefield. It collects and displays critical flight information from aircraft sensors and converts it into visual imagery. The system allows continuous "heads-up" flight without the need to continuously look down at the cockpit instrument panel.

The AHUD is an Advanced Electro-Optical System integrated with the Night Vision Goggle (NVG). The system senses critical flight data (i.e., altitude, airspeed, attitude, torque, compass heading) and transmits the data to the NVG. The data is overlaid on the NVG imagery to provide the pilot and copilot with integrated night scene and critical flight data symbology. This results in significant operational advantages and survivability enhancements when performing night missions.



The AHUD has designed, within its system, a Built-In-Test (BIT) capability that continually monitors the health of the AHUD system while it is powered on. The results of this BIT function (along with certain platform specific attributes) are stored into an internal log called the 'Fault Log'. In the past, this log could have been accessed and downloaded, but the Army had no way of utilizing the information to support the repair or the sustainment of the AHUD system.

SEC decided that this information was valuable for troubleshooting software problems and formulating Engineering Change Proposals for the support of the AHUD system. This information was also determined to be useful in diagnosing AHUD system hardware failures and associated platform specific stimuli problems.

The FLAP Development Process

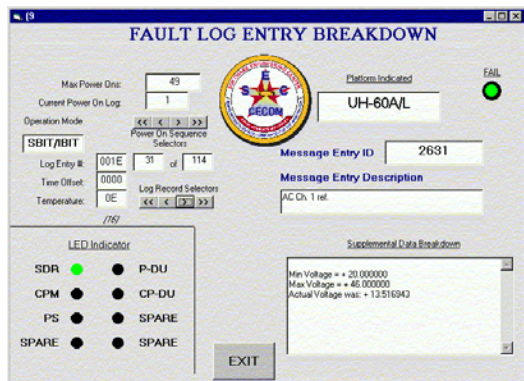
In its initial investigation, SEC found that there was no documentation drafted supporting this feature. The process to develop this tool would then require some reverse engineering, and SEC already had in place a team very experienced in troubleshooting and with reverse engineering computer based designs.

Normally, the process for developing a tool of this type would be to determine the format of the information stored, break it down, reformat and display the information; it was not to be that easy. Upon reviewing the Log code and the underlying BIT test module coding, it was determined that not only was there a format for the log itself, but every test involved also had its own format for the information stored. To

(cont'd next page)

FLAP (cont'd)

complicate this even further, the underlying hardware design used a memory storage method called 'Little Endian'. To simplify, 'Little Endian' takes the least significant byte of information and stores it in the most significant byte of memory for handling efficiency. The storage relationship changes even more if the write/read operation is a character (byte), word (16-bits), or a double word (32-bits) operation.



Sample LOG Entry Information Displayed

This arrangement caused SEC to examine and reverse engineer thousands of lines of code to map the entire process before beginning to design the FLAP tool. The tool was duly completed and tested on actual platform logs and will be available to Army units in their capacity to support the AHUD in both the field environment and the depot level environments.

The 'Fault Log Analysis Tool' is indicative of SEC's resources, experience and ability to support the Army's evolution as it enters the new century.

Submitted by Mr. Kwok Lo, CECOM SEC

'WARNING, WARNING WILL ROBINSON!'

Do you remember the robot on the TV program "Lost in Space" that was so eloquent and intuitive and could predict, identify and provide solutions to the problems faced by the intrepid space travelers? Well, like the robot, CECOM SEC Electronic Combat and I2WD are alerting and warning users of a possible anomaly with the AN/APR-39A(V)1/3/4 Radar Signal Detecting Set (RSDS). This anomaly can be encountered by the user when trying to reprogram a User Data Module (UDM) (with the DOS or EWOSS 2000 Memory Loader Verifier (MLV) software) and finds that the upload will not execute even after multiple attempts.



Old UDMs and new UDMs – look identical!

There are two probable reasons for this – one has been addressed before and that is the incompatibility of some of the newer and faster computers that do not effectively run the reprogramming software. Possible solutions to this were highlighted in the October 2001 issue of the "A/IEW Bulletin".

The other anomaly was first identified with a Foreign Military Sales (FMS) customer. The first clue to identifying the possible anomaly was that when the 'test' button was pressed, no built-in test took place, no Operational Flight Program 023.9 and no Mission Data Set (XXX) were displayed at the 12 and 6 o'clock

(cont'd next page)

Bad UDMs (cont'd)

positions on the IP-1150A display. The other indication was that when the MLV cable was attached from the laptop to the J-connector, no 'R' appeared in the center of the IP-1150A to indicate connectivity. No matter which MLV command sequence was activated, the only result in DOS was the repetitive display phrase 'SINGLE BYTE SENT'. In EWOS 2000, no 'R' appeared on the Windows display and no MDS could be uploaded.

After investigation and discussions with I2WD personnel, specifically Mr. John Reilly, it appears that UDMs purchased on a newer contract had been factory preset with a non-write code --- not permanent, but one that cannot be overwritten by the MLV software. These new UDMs and the older UDMS look alike, have the same part numbers and stock numbers, so finding them in our logistic system may be an immediate challenge.

We recommend that U.S. Army personnel work with your Logistic Avionics Representative (LAR) to verify that the UDM is the culprit. We recommend that the LARs call either Mr. Harinder Purewal at (732) 532-0291 (DSN 992) or Mr. John Reilly at (732) 427-2917 (DSN 987) for help in finding the most expeditious manner in which to replace the UDMs. If you are a USAF or USMC user, call either Mr. Purewal or Mr. Reilly for help. For FMS customers, it is recommended that the anomaly be reported as soon as possible to your Case Manager. The Army is attempting to correct this latent problem and hopes to have the logistic system purged in the near future.

Submitted by Mr. Peter McGrew, SRI International

The Army Battle Command System and What Capability it Brings to the Warfighter

Introduction

The Army Battle Command System (ABCS) is a "system of systems" being introduced to the Army to allow the Warfighters to:

- See the terrain
- See the enemy
- See the force

See the Terrain

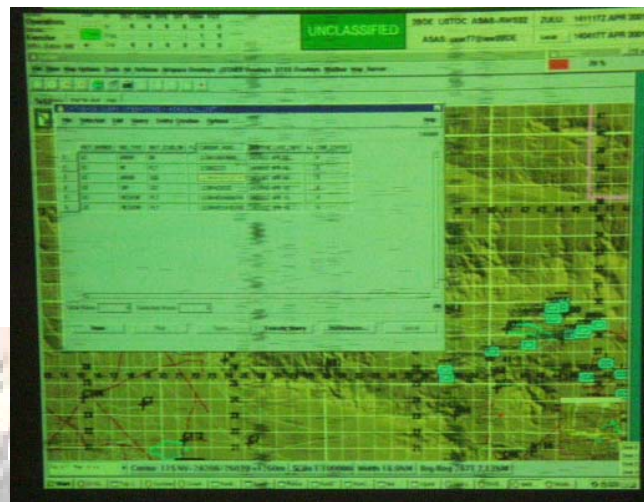
Seeing the terrain is implemented by the enabling systems, Digital Topographic Support System and the Integrated Meteorological System. These systems allow the Commander to see the slope, elevation, soil composition, erosion and weather conditions to determine the effects these factors will have on his plan.

(cont'd next page)

ABCS (cont'd)

See the Enemy

The Commander is able to see the enemy through the use of the All Source Analysis System (ASAS). ASAS receives electronic reports from multiple classified and unclassified sources and assists the analyst to fuse this information into an intelligence product. To the uninitiated, the collateral ASAS – Remote Workstation (RWS) is synonymous with the term ASAS. However, ASAS itself is a “system of systems” as much as ABCS is. The ASAS-RWS is able to provide the Maneuver Commander with a correlated “red” picture through the information it receives from the higher-level ASAS systems – such as the ASAS – All Source (AS), ASAS – Single Source (SS), and the ASAS – Communications Control Set (CCS). A welcome new arrival to the ASAS family is the ASAS-Light – a Windows NT based notebook computer that trades processing power for mobility. With the entire suite of ASAS systems, the unit’s Intelligence Officer is able to provide the Commander with timely and accurate predictive analysis.



See the Force

Although still in development, there are several systems within the Maneuver Battlefield Operating System that are approaching Initial Operational Test & Evaluation (IOT&E). These systems are the Force XXI Battle Command Brigade and Below (FBCB2) and the Maneuver Control System (MCS).

FBCB2 is the only ABCS system found at company, platoon and individual vehicle level. Coupled with the vehicle’s radio and the Global Positioning System, FBCB2 allows a Commander to see where his assets are in much the same way the National Training Center’s “Star Wars” screens do...except FBCB2 is capable of doing this on ANY terrain and is not installation dependent.



At the heart of ABCS is the MCS. By using the ABCS systems in the field, the Warfighter has determined that, because of the use of dynamic Internet Protocol (IP) addresses, the MCS must perform the role of the tactical operations center (TOC) boot server. When a unit TOC is moving into position to set up, the operations track – S-3 – is the first vehicle to move into position. All other vehicles adjust off of this vehicle. Therefore, since the S-3 track is the first to be emplaced, it is the first ABCS system to boot up. All other ABCS systems can then boot up and obtain an IP address from the TOC boot server.

(cont'd next page)

ABCS (cont'd)

Once operational, the MCS receives the live “blue” feed from the FBCB2 systems and the correlated “red” picture from the ASAS-RWS. Whether the Maneuver Commander chooses to display the Commander’s Tactical Picture via the UNIX based MCS – Heavy or the Windows NT based MCS – Light notebook computer is based on a Commander’s preference and availability of hardware. By merging information from the FBCB2 and ASAS-RWS on the “see-all” screen in the TOC, all members of the staff fight off the same “map” thus facilitating *dominant maneuver*.



Sensor to Shooter Linkage

One may ask, “The Commander can see all this information, but is it just to make decisions?” The answer is no. The staff can see the “big picture” and use it to place “steel on target” from the TOC by using the Advanced Field Artillery Target Data System (AFATDS). The ASAS-RWS sets parameters for target criteria so that when the system receives an electronic enemy observation report that matches these criteria, an automatic call-for-fire message is sent to the AFATDS. The AFATDS processes these messages and then prioritizes the fire missions according to guidance set forth by the Commander. Each fire mission is executed in sequence and sent down to the gun batteries for firing. This makes the most efficient use of artillery ammunition possible on the battlefield and places the right munitions at the right place at the right time.

Sustaining the Force

“An Army travels on its stomach” is a famous quote by Napoleon alluding to the importance of logistics. This axiom still holds true today. The “digital” Army is developing the Combat Service Support Control System to assist the Commander in tracking the status of all classes of supply for his forces. The logistician will be able to receive information from FBCB2 equipped systems and from Standard Army Maintenance Information Systems. This information will allow the logistical planners to support the Warfighters by using anticipatory logistics to deliver “just-in-time” supplies to the right place at the right time.

Conclusion

As the Commander sees the terrain, the red (the enemy), and the blue (themselves) on the same picture, he is able to make timely and accurate decisions on the employment of his forces, set the priority of fires and the priority of support to achieve his objectives and accomplish his warfighting mission. As these components of the ABCS systems pass their IOT&E, obtain full material release and transition to CECOM for Post Production Software Support, the Software Engineering Center stands ready to support them as the Army’s premier software sustainment organization.

(cont'd next page)



ABCS (cont'd)

For additional information, please contact:



United States Army Communications-Electronics Command
Software Engineering Center Intelligence Fusion Systems
Fort Huachuca, AZ 85613-5000
Phone (520) 538-6188; DSN 879-6188
<http://cecom-ifs.army.mil>



(Re)Introduction to Army Reprogramming Analysis Team Communications Services



It's been a while since we ran an article on the communications services that the Army Reprogramming Analysis Team (ARAT) provides to the Warfighter and those who support the Warfighter. Now, as our reader base grows across the entire BSSD community, we would like to take this space to acquaint our new readers with ARAT communications services. For our many readers who know what these services are and have taken advantage of what the ARAT has to offer, this will be a reintroduction to what we do.

ARAT Overview

The ARAT is a networked group of organizations from the Army's Communications-Electronics Command (CECOM) Software Engineering Center (SEC), Land Information Warfare Activity and Training and Doctrine Command, as well as Joint Services and Department of Defense (DoD) activities. Their mission is to support the Tactical Commander by providing timely reprogramming of operational software in Aviation Survivability Equipment (ASE). Essentially, the ARAT provides software changes, not readily possible by operator input, in response to rapid deployment or to changes in the threat environment.

The CECOM SEC's Electronic Combat Branch (ECB) specializes in providing systems engineering support related to reprogramming the Mission Data Sets (MDS) within ASE. These systems include radar signal detecting sets, laser detectors, radar jammers and missile countermeasure sets used on a variety of rotary wing, fixed wing and surface vessel platforms. Although MDSs are the essence of ASE systems, they do no good if they cannot reach the Warfighter, and it is the ECB's responsibility to ensure that they get to the field.

ARAT Communications Services

ARAT engineers play an active role in engineering, supplying and supporting an infrastructure of computer servers, networks and communication devices to allow Warfighters the capability of accessing mission critical data. This capability extends from remote dial-up capability to direct Secret Internet Protocol Router Network (SIPRNET) access. At the ECB, ARAT engineers have designed a system of servers and incorporated communication devices that allow remote Warfighters, such as Army Aviation Electronic Warfare Officers, to utilize NSA approved dial-up encryption devices such as the Secure Telephone Unit III (STU-III) and Secure Telephone Equipment (STE) to access ARAT generated information and MDSs.

(cont'd next page)

ARAT (cont'd)

Accounts and Access

The ARAT communications infrastructure has opened the doors both to services and information provided by the ARAT and to data produced by the National Intelligence Community. The following describes the various accounts available through the ARAT and the means to access them.

If you are a Warfighter and require access to the MDSs, Tactics, Techniques and Procedures and other related threat data files for your ASE, you will need to establish an account on the Multi-Service Electronic Warfare Data Distribution System (MSEWDDS). The MSEWDDS, located at Eglin AFB, FL, holds the MDSs and other files that you will need, and is structured with several mirror sites to ensure continuity of access. To access the MSEWDDS, you will first need to complete the “MSEWDDS Account Request Form”, which you can download from the Internet/NIPRNET ARAT web site.

For those who require additional intelligence data, or are looking for a more dependable and advantageous method to gain access to the MSEWDDS, you should turn to the SIPRNET. The SIPRNET is just like the Internet, except encrypted (thus secure) at the SECRET Collateral level. Also, just like the Internet, the SIPRNET has a World Wide Web known as INTELlink-S, which provides access to intelligence reports and information from a variety of National Intelligence Community agencies such as the National Imagery and Mapping Agency, the Defense Intelligence Agency and the National Ground Intelligence Center. You can access the SIPRNET through a direct drop at your location or via a direct dial-up SIPRNET account.

To establish a direct SIPRNET drop at your location, you will need to coordinate directly with the Defense Information Systems Agency (DISA). A direct drop has its advantages, but is a costly and time intensive effort that doesn't lend practicality to mobile Warfighters. For this, the alternative is to obtain an ARAT dial-up SIPRNET account.

As mentioned, the MSEWDDS site is accessible via SIPRNET/INTELlink-S through a link on the ARAT SIPRNET website. This link allows users to access the MSEWDDS via INTELlink-S SIPRNET web, provided they have an MSEWDDS account (userid and password). In addition, by attaining an ARAT SIPRNET account, you will also be able to exchange email with any other user on the SIPRNET.

To obtain an ARAT dial-up SIPRNET account, you will need to fill out an ARAT account form and fax it to the ECB (fax number can be found on the form). You will also need to send your clearance information from your S-2 and your computer's accreditation paperwork from your IMO/AMO/ISSO/TASO personnel. If you do not have an ARAT account form, you can download it from the Internet/NIPRNET ARAT web site at URL:

Forms URL:

http://arat.iew.sed.monmouth.army.mil/ARAT/ARAT_information/forms/account_forms/forms.htm

(cont'd next page)

ARAT (cont'd)

ARAT NIPRNET Web Site URL:

<http://arat.iew.sed.monmouth.army.mil>

Note: If you are unable to access or download any of the forms mentioned above, call one of the POCs listed at the end of this article and they will either fax or mail it to you.

Once you have completed all of the necessary paperwork and received approval from the ARAT, you will need to have the following hardware and software, at a minimum, to gain dial-up access to the MSEWDDS or the SIPRNET:

- STU-III/STE: The STU-III will need to have the capability of data rate transfer at a minimum of 9600 bps, preferably 38400 bps. The ARAT recommends a Motorola SECTEL 1500, or AT&T (Lucent, General Dynamics) 1100 or 1910, or an L-3 Communications STE. Be aware, however, that you can no longer purchase the STU-III, as DoD is phasing it out of its inventory. See the July 2001 issue of the "A/IEW Bulletin" for details on replacement technology to the STU-III.
- TCP/IP/PPP: Software such as Microsoft's Trumpet Winsock (Transmission Control Protocol/Internet Protocol/Point-to-Point Protocol) which is included in Windows 95, 98 and NT.
- Web browser software (e.g., Netscape or Microsoft Internet Explorer).

ARAT has been involved in trying to incorporate the Palladium/RASP product as part of the suite of dial-up devices offered to the Warfighter. The Palladium is a PCMCIA type device that NSA has accredited to the SECRET level, and that DISA approved as a SIPRNET dial-up device. The Palladium is a very inexpensive device that offers its users enhanced dial-up capability with a 33.3 kbps baud rate, with excellent error correction capability on DSN lines. For further information regarding ARAT's attempt to incorporate the Palladium into the ARAT SIPRNET dial-up suite, or to learn more about the device, see the July 2001 issue of the "A/IEW Bulletin" or go the Palladium website (www.rasp4secret.com).

ASE Reprogramming Support

Connectivity is only part of the ASE reprogramming process. Once you have obtained the MDS file, you will need to program that MDS into your ASE. To do so, you will need the following equipment and software:

- ARAT Memory Loader/Verifier (MLV) Kit. This kit contains the cable needed for reprogramming. You can request the kit by filling out the MLV Reprogramming Kit Request Form at:

http://arat.iew.sed.monmouth.army.mil/ARAT/ARAT_information/forms/MLV_request/mlv_request_form.htm

(cont'd next page)

ARAT (cont'd)

- Reprogramming software, EWOSS 1.0.5 (Windows) or MLV (DOS). This software is on the *ARAT Toolbox CD* (see below) or can be downloaded from the ARAT NIPRNET or SIPRNET sites at:

http://arat.iew.sed.monmouth.army.mil/ARAT/ARAT_information/Software/arats_software_library.htm

- Computer: A newly developed version of EWOSS, Version 1.0.5 has been developed and tested that now enables the software to operate successfully on Windows 95, 98, NT and Windows 2000. The EWOSS software will also operate on Pentium I-IV laptops and computers. Any questions concerning Version 1.0.5 can be directed to the ARAT help desk (732-532-9395, DSN 992-9395). Obtaining a computer (preferably a laptop) is the user's responsibility, but the ARAT can assist you in locating surplus computers that may fulfill your needs.

Additional Support

The success of the ARAT has been our ability to assist the Warfighter before, during and after the ARAT account process. Our engineers are available to respond to user needs and problems and, if necessary, talk you through any of the processes until the issue is resolved. Our support team, formed in the early 1990's and tested during Operations "Allied Forces" and "Enduring Freedom", can assist with questions concerning paperwork, software, hardware and communication technical questions or issues.

You can contact the ARAT Communications Infrastructure Support Staff at:

DSN: (312) 992-9392/9395/0582 or Commercial: (732) 532-9392/9395/0582

Contacts: Mr. Mike Crapanzano (Michael.Crapanzano@mail1.monmouth.army.mil)
Mr. Marc Demarest (Marc.Demarest@mail1.monmouth.army.mil)
Mr. Eric Lee (Eric.Lee@mail1.monmouth.army.mil)

For MSEWDDS specific assistance, contact Mr. Robert Hankins at (312) 872-2166 (DSN) or (850) 882-2166 (Commercial) (Email: Robert.Hankins@eglin.af.mil)

ARAT also offers and supplies an *ARAT Toolbox CD* that contains all of the account forms, software and documentation needed to obtain, configure and access an ARAT SIPRNET dial-up account. You can request the CD via the Internet at:

http://arat.iew.sed.monmouth.army.mil/ARAT/ARAT_information/forms/CD_request/cd_request_form.htm

Another service available to ARAT users is the "Battlespace Systems Directorate (BSSD) Bulletin". This bulletin began as the "ARAT Bulletin" in 1994 then migrated to become the "Avionics/Intelligence and

(cont'd next page)

ARAT (cont'd)

Electronic Warfare Bulletin" in 2000. Today's "BSSD Bulletin" provides insight into a variety of systems supported by the CECOM SEC while maintaining a focus on issues of particular interest to the ASE community. Warfighters interested in receiving this quarterly bulletin should contact the ECB.

Previous bulletins are available for review and download at the ARAT website at:

<http://arat.iew.sed.monmouth.army.mil> (click on the *information*, and then *bulletin* links to access this archive.)

One important note on the "BSSD Bulletin" - this is your publication as much as it belongs to the BSSD. We need your input, especially articles about lessons you've learned that will benefit other Warfighters.

Summary

The ARAT has much to offer to the Warfighter, especially those in the ASE community. The ARAT staffs at the ECB and Eglin AFB stand ready to provide assistance for any Warfighter requiring the ARAT services.

If you require our services, remember these key points:

- If you require access to the MSEWDDS via dial-up and/or via the ARAT SIPRNET, you must provide the necessary information to the MSEWDDS staff at Eglin AFB, FL, regardless of the method of access you are going to use.
- If you require access to the MSEWDDS and dial-up SIPRNET access, you will need to fill out an MSEWDDS account form (see above bullet) and also provide a completed ARAT dial-up SIPRNET account form, your security clearance and computer accreditation information to the ARAT at Fort Monmouth, NJ.
- All the necessary forms/memos and examples are available for downloading from the ARAT Internet/NIPRNET web site at the following URL:

http://arat.iew.sed.monmouth.army.mil/ARAT/ARAT_information/forms/account_forms/forms.htm

- The MSEWDDS administrative staff at Eglin AFB, FL handles the MSEWDDS accounts, and the ARAT staff at Fort Monmouth administers dial-up SIPRNET access accounts. The Fort Monmouth staff can also assist you in contacting and forwarding your MSEWDDS paperwork to the MSEWDDS staff, but not in creating the actual MSEWDDS account.

For additional information about the ARAT, visit the CECOM SEC's ARAT website at:

<http://www.sed.monmouth.army.mil/c4iews/araf/>

Submitted by the ARAT Team, Fort Monmouth

For Your Information

Coming Events!

<i>Event</i>	<i>Location</i>	<i>Date(s)</i>
<i>Space & Missile Defense Symposium & Exhibition</i>	<i>Judson F. Williams Convention Center El Paso, TX</i>	<i>10-12 December 2002</i>
<i>Aviation Symposium & Exhibition</i>	<i>Fairview Park Marriott, Falls Church, VA</i>	<i>6-8 January 2003</i>
<i>AUSA Winter Symposium</i>	<i>Broward County Convention Center Ft. Lauderdale, FL</i>	<i>26-28 February 2003</i>
<i>2003 AAAA Annual Convention</i>	<i>Fort Worth, TX</i>	<i>9-12 April 2003</i>
<i>FiestaCrow 2003</i>	<i>San Antonio, TX</i>	<i>20-23 April 2003</i>
<i>Logistics Symposium</i>	<i>Richmond, VA</i>	<i>22-24 April 2003</i>

Now Available on the Web

All 25 previous issues of the "ARAT Bulletin", "A/IEW Bulletin" and "BSSD Bulletin" are now available on the ARAT web site. The issues are available in HTML format for on-line viewing, as well as in PDF and MS Word 97 format for viewing and downloading.

Future issues will also be posted on the site and in the same format. You are encouraged to download any issue (or issues) for local reproduction and distribution within your agency.

The ARAT web site can be accessed at <http://arat.iew.sed.monmouth.army.mil/>, or from a link on the A/IEW web site at <http://www.iew.sed.monmouth.army.mil/>

ATTENTION ELECTRONIC WARFARE OFFICERS!

Electronic Warfare Officers requiring Memory Loader/Verifier (MLV) reprogramming kits, copies of the "ARAT Software and Documentation Toolbox" CD or the "Mission Data Set Training" CD should contact either Mr. John Amoretti (DSN: (312) 992-0303/CML: (732) 532-0303) (john.amoretti@mail1.monmouth.army.mil) or R²CIL (DSN: (312) 992-9395/9392/CML: (732) 532-9395/9392) (webmaster@arat.iew.sed.monmouth.army.mil) or fax your requests to DSN: (312) 992-8287/5238 or CML: (732) 532-8287/5238.

Help Us Help You

If you are moving, have moved, or your address is listed incorrectly on the mailing envelope, please call Ms. Kimberly Weaver at (732) 532-5324 or email at Kimberly.Weaver@mail1.monmouth.army.mil with the correct address. Many Bulletins are returned for incorrect addresses and unknown addressees. We would like to reduce the amount of returned mail and ensure that all of our customers receive the latest issue of the "BSSD Bulletin". Thank you for your support.

ARAT Rapid Reprogramming Communications Infrastructure Laboratory (R²CIL)

Telephone:

#1 (732) 532-9395

DSN: 992-9395

#2 (732) 532-9392

DSN: 992-9392

#3 (732) 532-0303

DSN: 992-0303

#4 (732) 532-5319

DSN: 992-5319

Answering machine/voice mail option is available at these numbers for after-hour messages

Email:

Unclassified:

webmaster@arat.iew.sed.monmouth.army.mil

monmouth.army.mil

SIPRNET:

webmaster@arat.army.smil.mil

The Battlespace System Support Community Key Points of Contact

Agency	Name/e-mail	Comm/DSN	Fax Number
Director, (A), Battlespace Systems Support	Mr. M. Leonard Katz myron.katz@mail1.monmouth.army.mil	(732) 532-1825 DSN 992-1825	(732) 532-3538 DSN 992-3538
Deputy Director, (A), Battlespace Systems Support	Mr. Joseph Ingrao joseph.ingrao@mail1.monmouth.army.mil	(732) 532-0065 DSN 992-0065	(732) 532-3538 DSN 992-3538
Chief, A/IEW Division	Mr. William Walker william.walker@mail1.monmouth.army.mil	(732) 532-6253 DSN 992-6253	(732) 532-8287 DSN 992-8287
Chief, COMM Division	Mr. Jeffrey Downing jeffrey.downing@mail1.monmouth.army.mil	(732) 532-5163 DSN 992-5163	(732) 532-3065 DSN 992-3065
Intelligence Fusion Branch	Mr. Medhat Abuhantash medhat.abuhantash@cecomifs.hua.army.mil	(520) 538-6188 DSN 879-6188	(520) 538-7673 DSN 879-7673
Chief, Fire Support	Mr. Eugene Crostley crostlef@fssec.army.mil	(580) 442-3350 DSN 639-3350	(580) 248-8661
ESSO	Mr. Steven Cooper steven.cooper@hq.amceur.army.mil	49-621-487-3708 DSN (314) 375-3708	49-621-487-7635 DSN (314) 375-7635
KSSO	Mr. John Franz franzj@usfk.korea.army.mil	DSN (315) 741-6094	DSN (315) 741-6582
Chief, ARAT-TA (Eglin AFB)	Mr. Christian Gilbert christian.gilbert@eglin.af.mil	(850) 882-8899 DSN 872-8899	(850) 882-9609 (C) -4268 (U) DSN 872-9609 (C) -4268 (U)

The BSSD Bulletin Staff

Editor-In-Chief
Mr. Joseph Ingrao, BSSD

Editor
Mr. John Hakim

Distribution Manager
Ms. Kimberly Weaver, BSSD

Send comments, changes of address, and articles to:

U.S. Army CECOM
Software Engineering Center
ATTN: AMSEL-SE-WS-AI
Fort Monmouth, NJ 07703
FAX: (732) 532-5238
DSN 992-5238